Microsoft Windows XP Service Pack 2 Default Security Features

8/2/2004

Purpose:

This paper will discuss the possible adverse implications for Applications, caused by new feature default settings, when installing Windows XP Service Pack 2.

Discussion:

Microsoft will shortly be releasing Windows XP Service Pack 2. With this release, it is attempting to strengthen the default security settings for XP and make it "Secure out of the box".

While this will provide increased security for many home users of the product who probably have not taken advantage of the built-in security features of XP, it may introduce some problems for DOD sites who are running critical applications and may have implemented third party security products on the XP systems.

This paper will discuss only the potential impact for existing applications that will be caused by the default security settings and features that are implemented upon installing Service Pack 2. The discussion is based upon Service Pack 2 RC1, which Microsoft released for testing purposes. Microsoft is addressing some of the concerns reported, related to application incompatibility, so there may be some changes in the final Service Pack release.

The following security features will be enabled by default when Windows XP Service Pack 2 is installed, and have the potential of adversely impacting some existing applications.

1. RPC Interface Restriction – Microsoft made changes to the Remote Procedure Call service to make it more secure. They created a new RestrictRemoteClients registry key, whose default setting will reject all anonymous RPC calls. If an existing application expects to receive calls from remote anonymous RPC clients, this may break the application.

2. Windows XP was originally released with a built-in Internet Connection Firewall (ICF) that had to be enabled and configured by the User to be effective. With Service Pack 2, Microsoft has added additional functionality to ICF and renamed it to "Windows Firewall". It is enabled by default when Service Pack is installed. It will permit all outbound connections, but applies rules to communications that come back into the computer. This may break application compatibility if the application does not work with stateful filtering by default. It may also conflict with other active software and hardware firewalls. By default RPC will not function through the Windows Firewall. All services and applications that use RPC are affected. However, the firewall can be configured to permit RPC.

3. Execution Protection (NX) – This feature marks all memory locations in a process as non-executable unless the location explicitly contains executable code. Some application's behaviors are expected to be incompatible with execution protection.

4. Wireless Access – There is an existing vulnerability in Windows XP, if a wireless NIC card is installed, in that the system will automatically search for an existing hotspot and attempt to connect. Information can be passed in unencrypted format and be exposed to interception. Microsoft has introduced Wireless Provisioning Services in Service Pack 2 in an attempt to control this process and encrypt the authentication information being passed in setting up a connection.

   WPS allows a user to be authenticated to a wireless network (e.g. wireless hotspot or DoD WLAN). If the user has the correct authentication credentials, the access point will direct the user to a VLAN where they will get access to those wireless services assigned to their account. WPS handles this process automatically for the user. If the user does not have the correct authentication credentials, the user will be directed to another VLAN by the access point where they can enter credit card info to obtain a valid account (and authentication credentials).

   In the DoD environment, where each user needs to use strong authentication and FIPS 140-2 certified encryption, WPS will not work and should be turned off. An exception would be for those DoD wireless users who are on travel and want to connect to a WLAN hotspot to connect to the Internet and VPN into a DoD network. In this case WPS will simplify (automate) the process of connecting to the hotspot access point and authenticate to the Wireless Internet Service Provider (WISP).

The new security features that have been addressed are those that are enabled by default when Service Pack 2 is installed. Microsoft has introduced additional features that are not enabled by default, but are designed to provide additional security. Much of the information here was derived from a white paper from Microsoft "Changes to Functionality in Microsoft Windows XP Service Pack 2" that describes the new features and their potential impact on applications, as well as fixes for any problems encountered. It is available at http://www.microsoft.com/downloads/details.aspx?FamilyID=7bd948d7-b791-40b6-8364-685b84158c78& displaylang=en

Conclusion:

Sites need to be aware of the possible adverse impact on existing applications when installing Windows Service Pack 2. SA's and application developers should review existing applications beforehand to try to identify potential problem areas. Sites that use third party firewalls on the Windows XP systems should plan on disabling Windows Firewall when SP2 is installed.